

DEPARTMENTAL REGULATION		Number: 3040-001
SUBJECT: Electronic Records Management Program	DATE: April 7, 1993	
	OPI: Information Management Division, Office of Information Resources Management	

1 PURPOSE

This regulation prescribes the policies, responsibilities, and procedures for the management of electronic records within the Department of Agriculture. It also establishes the basic requirements related to the creation, and maintenance, adequate documentation, and proper records disposition of electronic records, which include all data files and data bases as well as text information in an office automation system. Unless otherwise noted, these requirements apply to all electronic records systems, whether on microprocessors, mini- or mainframe computers, regardless of storage media, in network or stand-alone configurations. This directive is designed to help managers carry out their responsibilities and at the same time establish and maintain an active, continuing program for the economical and efficient management of electronic records consistent with the policies established by the General Services Administration and National Archives and Records Administration.

2 REFERENCES

- a National Archives and Records Administration General Records Schedule, GRS 20, Electronic Records.
- b National Archives and Records Administration Bulletin, 87-5, Electronic Recordkeeping.
- c National Archives and Records Administration - Managing Electronic Records (An Information Package, 1986).
- d Chapters 21, 29, 31, and 33 of Title 44, U.S. Code.
- e General Services Administration Electronic Recordkeeping Handbook, October, 1987.
- f Departmental Regulation 3130-2, Microcomputer Policy.

- g Departmental Regulation 3140-1, USDA ADP Security Policy.
- h Departmental Manual 3140-1, ADP Security Manual.
- i 36 CFR 1234-2 Definitions.
- j 36 CFR 1234-10, Program Requirements
- k 41 CFR Part 201-45, Management of Records
- l OMB Circular A-130, 8a (1), Management of Federal Information Resources (December 12, 1985).
- m Computer Security Act of 1987 (P.L. 100-235).
- n Section 2071 of Title 18, U.S. Code.
- o FIRMR Bulletin C-8, Information Accessibility for Employees with Disabilities.
- p Justice Department "A Guideline for Federal Records Managers or Custodians."

3 ABBREVIATIONS

- DM - Departmental Manual
- DR - Departmental Regulation
- FRC - Federal Records Center
- GAO - General Accounting Office
- GSA - General Services Administration
- NARA - National Archives and Records Administration
- OIRM - Office of Information Resources Management
- OGC - Office of the General Counsel
- SCSI - Small Computer System Interface
- USDA - United States Department of Agriculture
- WORM - Write Once, Read Many

4 POLICY

All records, including those in electronic form, will contain adequate and proper information regarding the functions, organizations, policies, procedures, decisions, and essential transactions they are intended to document; be sufficient to protect the legal and financial rights of the Government; be easily retrievable and usable; be protected from unauthorized access, loss, removal, or theft; be protected from unauthorized disclosure; and be disposed of only in compliance with NARA-approved records control schedules.

5 DEFINITIONS

- a Byte. A unit of information for processing in certain kinds of electronic computers, equal to one character or eight bits.
- b Computer Accommodation. The acquisition or modification of Federal Information Processing (FIP) resources to minimize the functional limitations of employees in order to promote productivity and to ensure access to work-related information resources.
- c Data Base. A set of data consisting of at least one data file, that is sufficient for a given purpose.
- d Data Base Management System. A software system used to access and retrieve data stored in a data base.
- e Data File. Related numeric, textual, or graphic information that is organized in a strictly prescribed form and format.
- f Digital Data. Information captured/stored as discrete, off-and-on signals.
- g Digital Image. An electronic data file consisting of digital data, that when reconstructed either on a display screen or hard copy print, appears as the original document.
- h Electronic Record. Any record that is created, used, maintained, transmitted, and disposed of in electronic form. Such records may be stored in computer memory (random access memory) or on flexible disks. Offices may or may not have non-record paper copies of electronic records. Electronic records are also referred to as machine-readable records because they require machine processing for conversion to human-readable form. Examples of these types of records include those on magnetic tapes, disks and drums, video files, optical disks, and floppy disks.
- i Electronic Recordkeeping. The creation, maintenance, use, and disposition of records created and stored by using a computer.
- j Electronic Record System. Any information that produces, manipulates, or stores Federal records by using a computer. A system of electronic records having the same physical form and one or more of the following aspects: arrangement under a single filing system,

relation to a particular subject, documentation of a particular kind of transaction, and production by the same activity.

k Electronic Records Management. The planning, budgeting, organizing, directing, training, and control activities associated with electronic records.

l Handicapped Individuals or Individuals with Disabilities. Qualified individuals with impairments, as cited in 29 CFR 1613.702(f), who can benefit from electronic office equipment accessibility.

m Index. Descriptive information attached to a file that enables a requestor to identify the file and retrieve it from the storage medium.

n Information Accessibility. The application or configuration of FIP resources in a manner that accommodates the functional limitations of individuals with disabilities so as to promote productivity and provide access to work-related or public information resources.

o Information Systems. The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

p Jukebox. Descriptive term applied to optical disk storage systems which utilize robotic devices containing shelves and automated picking mechanisms to store multiple disks and provide automatic digital image delivery.

q Laser Printer. Commonly used in electronic imaging systems, this non-impact device utilizes laser beams to create a temporary image on a photosensitive material. This latent image is developed by applying toner particles, which is subsequently transferred and permanently fused to create the paper print.

r Megabyte. One million bytes.

s Non-Record Material. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience or reference, and stocks of publications and processed documents. May include:

- o Reading file copies of correspondence.

- o Tickler, follow-up, or suspense copies of correspondence.

- o Identical duplicate copies of all documents maintained in the same file.

- o Extra copies of printed or processed materials, official copies of which have been retained for record purposes.
- o Superseded manuals and other directives maintained outside the office that is responsible for retaining them.
- o Materials documenting such peripheral activities of agencies as employee welfare activities and charitable fund drives.
- o Routing slips.
- o Working papers.
- o Drafts of reports and correspondence.
- o Transmittal sheets.
- o Blank forms.
- o Transcribed stenographic materials.
- o Processed or published materials that are received from other activities or offices and that require no action and are not required for any kind of documentation (the originating office or activity is required to maintain record copies).
- o Catalogs, trade journals, and other publications or papers that are received from Government agencies, commercial firms, or private institutions and that require no action and are not part of a case upon which action is taken.
- o Correspondence and other records of short term value that, after action has been completed, have neither evidentiary nor informational value, such as requests for publications and

communications on hotel reservations.

- o Reproduction materials, such as stencils, hectograph masters, and offset plates.

- o Information copies of correspondence and other papers on which no documented administrative action is taken.

- o Physical exhibits, artifacts, and material objects lacking documentary values.

t Record Material. Records are books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.

u Rewritable Disk. An optical disk that, unlike WORM Disks can be erased, written over, and otherwise reused. Both magneto-optical and phase change technology is currently used.

v Special Peripheral. Is defined in Section 508 of P. L. 99-506 as "a special needs aid that provides access to electronic equipment that is otherwise inaccessible to a handicapped individual."

w Text Documents. Narrative or tabular documents, such as letters, memorandums, and reports, in loosely prescribed form and format.

x WORM Disk. An acronym for Write-Once, Read-Many times optical disks which can store user data (write) and can be accessed (read) when needed. The data recorded on WORM disks is considered permanent, in that the disks are not erasable/reusable like conventional magnetic media.

6 RESPONSIBILITIES

a The Information Management Division, Office of Information Resources Management, has overall responsibility for the Department-wide electronic records management program. The Information Management Division:

- (1) Develops policies, procedures, and guidelines to improve the effectiveness of the USDA electronic records management program.
- (2) Provides assistance and advice to agencies and staff offices on electronic records management matters.
- (3) Acts as liaison with NARA on overall direction of the Department's electronic records management program.
- (4) For staff offices, acts as liaison with NARA on scheduling, transferring, and disposing of electronic records.
- (5) In cooperation with the Planning, Review, and Standards Division, or on its own initiative directs, coordinates, or conducts reviews of USDA agency and staff office electronic records management programs.
- (6) Represents the Department in matters relating to electronic records management.
- (7) Coordinates electronic records management with other areas of information management.
- (8) Maintains a complete and accurate inventory of all electronic record systems.

b Agencies and Staff Offices will:

- (1) Assure that their organizations have established an electronic records management program in conformity with this regulation.
- (2) Manage, control, and coordinate all electronic records management activities within their organization through their Records Managers.
- (3) Prevent the loss of information from electronic records because of deterioration of the records medium. As an example, information can be preserved by rewriting it on another medium.
- (4) Schedule the disposition of all electronic records (including those created and maintained for the Government by a contractor) as well as related documentation and indexes, as soon as possible but no later than one year after their implementation.

- (5) Ensure that electronic records are preserved and disposed of in accordance with agency records disposition schedules.
- (6) Provide for the accession of permanent electronic records by NARA based on the records media and format prescribed by NARA.
- (7) Recycle records storage media, such as magnetic tapes, when possible, to reduce the costs of purchasing additional records storage media.
- (8) Install economical methods for procuring and storing supplies needed for the operation of electronic recordkeeping systems.
- (9) Provide training for users of electronic recordkeeping systems in the operation, care, and handling of system equipment, software, and media.
- (10) Develop security controls to prevent the unauthorized alteration or erasure of information in electronic records.
- (11) Implement systems for backing up electronic records that safeguard against loss of records information because of equipment malfunctions or human error.
- (12) Maintain an inventory of electronic record systems (see section 16), specifying the location, manner, and media in which electronic records systems are maintained to meet operational and archival requirements.
- (13) Establish procedures to ensure that contractors deliver to the agency those data files, data bases, and related documentation that are necessary to provide adequate and proper documentation of agency functions, policies and activities, and to protect legal and financial rights of the Government and of persons directly affected by the agency's activities (see 44 U.S.C. 3101).
- (14) Maintain adequate and up-to-date technical and informational documentation for data files and data bases. Minimum documentation required is a narrative description of the system; physical characteristics; recording mode information, including the coding structure (code books); recording system information; and a record layout that describes each field including its name, size, starting or relative position, and a description of the form of the data (such as alphabetic, zoned decimal,

packed decimal, or numeric), or a data dictionary or the equivalent information associated with a data base management system including a description of the relations between data elements in relational data bases.

c Agency Records Managers will:

(1) Establish appropriate policies and procedures establishing their own internal electronic records management programs to ensure that electronic records and their documentation are retained as long as needed. A copy of these directives should be sent to the Information Management Division, OIRM.

(2) Assure that agency electronic records as well as related documentation and indexes are properly scheduled and removed from office space and equipment in a timely manner.

Agencies will deal directly with NARA on scheduling, transferring, and disposing of agency electronic records.

(3) Provide assistance and advice to agency personnel on electronic records management matters.

(4) Evaluate the electronic records management activities of subordinate offices.

d Staff Office Record Managers will coordinate with the Information Management Division, OIRM, on all matters relating to electronic records management.

e Program Managers who currently manage or plan to develop an electronic record system are responsible for ensuring that these requirements are implemented for their systems. Program Managers will coordinate electronic records systems activity with their Records Managers to:

(1) Identify the office of primary interest for the records being created.

(2) Determine if the material being created is record or nonrecord.

(3) Determine in what form the official record will be maintained for its life cycle; i.e., paper, microform, tape, disk or diskette.

(4) Specify the method of implementing controls over national security classified, sensitive,

proprietary, and Privacy Act records stored and used electronically.

(5) Establish procedures for identifying, cataloging, and labeling electronic records when they are created.

(6) Establish an appropriate filing and retrieval system.

(7) Apply appropriate disposition instructions to electronic records.

(8) Ensure that adequate system documentation is created and maintained for as long as the related records exist.

f All employees will:

(1) Maintain electronic records according to prescribed agency policies and procedures.

(2) Safeguard electronic records until they are authorized for disposition. The unauthorized removal, concealment, falsification, mutilation, and/or unauthorized disposition of official records is prohibited by law and is subject to penalty (Section 2071 of Title 18, U.S. Code).

(Electronic records are to be treated the same as paper records, that is, their maintenance and disposal must be approved by the National Archives.)

(3) Notify agency records management personnel when unscheduled electronic records are identified.

(4) Submit electronic records to authorized personnel when leaving any position in the Federal Government.

7 SPECIAL CHARACTERISTICS OF AN ELECTRONIC RECORDS MANAGEMENT PROGRAM

a Without proper management, important electronic records can be lost, erased, misplaced, damaged, or otherwise disposed of prematurely. Similarly, records maintained in electronic form are subject to being retained for longer than authorized periods because they take up relatively little space (NARA Bulletin 87-5, Attachment A, #6). Either situation should be avoided.

b The technologies used in electronic recordkeeping, including telecommunications systems, make it easy to create new files, and

access and manipulate existing files from both local and remote terminals. Employees must be aware that they may be violating Federal regulations if they establish or change agency information systems, or change access methods to, or users of, existing systems without having the system design or design change reviewed and approved for records management considerations. See DM 3140-1 for guidance.

c Developers of electronic information systems must work closely with their respective Records Managers to determine whether the information being captured and used in the system is record material or nonrecord material, to insure that records disposition is handled appropriately, and to build proper safeguards into the systems for which they are responsible. Early involvement of Records Managers is especially critical in the case of major systems that may contain permanent records.

d Caution must be used when changing from one type of electronic information equipment to another or from one brand to another. Responsible agency officials must ensure that all essential information which requires updating and readability, including any information stored elsewhere, is converted to the new type of equipment.

8 NONRECORD AND RECORD INFORMATION IN ELECTRONIC FORM

a Creators and users of information in electronic form must be aware, prior to its creation and maintenance, whether the information is record material which requires a predetermined authorized life cycle, or is nonrecord material which may be disposed of after it has served its purpose, and must manage that information accordingly.

b The determination of record vs. nonrecord electronic records is based on similar criteria used for paper. If electronic records serve as the official record of correspondence, files, reports, and other official information, then they must be managed as record material. As such, the electronic record system must be appraised as a records series and the information retained in accordance with authorized records management practices.

c Nonrecord material in electronic form includes:

(1) Informational material that is maintained electronically on word processing diskettes and similar magnetic media used in the process of transcription, which has been produced in hard copy form for recordkeeping purposes, and which is retained in electronic form only to facilitate updating or revision of the material at a later date.

(2) Informational material which is a duplicate copy of record or nonrecord material on an electronic storage medium and is retained on the same or different type of electronic storage medium.

(3) Work papers and personal notes in electronic form that have no record value because they are meaningless to persons other than the individual who authorized them; provide no rationale, sense of direction, or guidance beyond and above that documented in official files; and generally are used only by the author to facilitate the development and finalization of papers for approval by appropriate officials.

(4) Miscellaneous informal electronic mail messages that do not contain information on, nor result in, and cannot be construed to imply policy of any element of the agency and have not been placed in the official files.

d Record material in electronic form includes:

(1) Informational material created or maintained only in electronic form, and never produced in hard copy form.

(2) Electronic mail messages, the contents of which concern statements of policy, rationale for a decision, sense of direction, or guidance above and beyond that documented in official files. Many electronic mail systems automatically erase information after the recipient has read it or within a short time span. Therefore, electronic records which are record material may need to be maintained in a medium that will satisfactorily store the record until its disposition date.

(3) The output of electronic information systems which support agency management functions, such as loan programs, commodity programs, and correspondence control systems, regardless of whether all or a portion of the information is generated electronically is also maintained in hard copy.

(4) Extracts of electronic information systems maintained in electronic form for the purpose of conducting studies and statistical analyses.

(5) Any electronic information file, regardless of its size, which contains personal information on individuals, the records for whom are retrieved by a unique personal identifier such as name or an assigned number.

e Currently, NARA accepts electronic records for accessioning into the National Archives of the United States only on one-half inch, seven or nine track reel-to-reel magnetic tape. Agencies can continue to

use reel-to-reel tape for storage and transfer. However, a growing number of Federal agencies are storing electronic records on 3480 class tape cartridges. After carefully evaluating this situation, NARA has concluded that 3480 class tape cartridges are a reliable storage medium for permanent electronic records.

Agencies are authorized to transfer permanent electronic records to the National Archives on 3480 class tape cartridges that meet the American National Standard based on the IBM format. The magnetic tape and cartridge for information interchange must be 18-track, parallel, 12.65 mm (1/2 inch), and 1491 cpmm (37,871 cpi).

All maintenance requirements of 36 CFR 1234.28(g) apply to 3480 class tape cartridges.

NARA will copy the contents of 3480 class tape cartridges at the time of accessioning and return them to the agency unless the agency indicates that it does not want the cartridges returned.

f Electronic records differ from records on other media in that the media on which electronic records are usually recorded are erasable, reusable, and used for rapid manipulation of data. This characteristic allows for economic creation of a variety of updated outputs tailored to specific needs.

g The media on which electronic records are recorded are fragile. Therefore, these records must be protected early in their life cycle. Ideally, protection should start when a system is created and the first records are entered.

h If the records to be maintained in the system contain information about individuals, and can be retrieved by the individual's name or other personal identifier, such as Social Security number, the records will be subject to the Privacy Act of 1974. The Privacy Act Officer should be contacted for requirements on documenting and publishing a description of the system of records.

i If the records to be maintained in the system contain proprietary data or information about individuals, or are deemed sensitive, the system design must include adequate safeguards to protect against unauthorized access and disclosure.

j Ensure that electronic records support internal control procedures as outlined in OMB Circular A-123 Revised, dated August 4, 1986, PL 97-255, Federal Managers' Financial Integrity Act of 1982, and PL 101-576, Chief Financial Officers Act of 1990.

Records relating to the development of fiscal policy should not be confused with records involving fiscal transactions. Fiscal policy files may have permanent value.

Digital imaging and optical media storage are rapidly evolving technologies, marked by the nearly continuous development of new approaches to converting, storing, and retrieving document images. Agencies using the technology for the storage and retrieval of records that are expected to exceed a system life of seven to ten years must ensure that their records retention needs are met.

Management Issues

The most fundamental management issue for archivists, records managers, and systems managers concerned about long-term records retention is maintaining access over time to image data stored on optical platter systems. Access to electronic records in general, including optical imaging systems, involves ensuring continuous readability and intelligibility.

Readability in an optical systems context means that the images can be processed on a computer system or device other than the one that initially created them or on which they are currently stored. Typically the lack of readability involves some incompatibility within the storage system/devices or an inability of the system to read the coding of image data from another system. Intelligibility, in contrast, means that the information is comprehensible to a human being.

The long-term viability of digital imaging and optical media storage systems is constrained by their current incapability of retaining content, context, and functionality over time. These limitations are driven primarily by three considerations:

- a vendor instability
- b system obsolescence (hardware/software)
- c media longevity

Vendor Instability. It is in the nature of manufacturer-vendor behavior that short term customer benefits take precedence over their long term needs, however clearly defined. It is incumbent upon systems decision-makers to assess carefully the viability of vendors when acquiring optical systems that are heavily vendor or manufacturer dependent. In lieu of ready made guarantees of long-term corporate stability, agencies are exploring the option of having proprietary vendor and manufacture computer codes placed in a secure accessible location in case of corporate failure.

System Obsolescence. It now seems apparent that optical media are far more durable and stable than the hardware and software required to maintain access. This argues strongly for a very proactive approach to both routine system maintenance and periodic system upgrade to preserve the usability of the system as a whole. In data centers, managers generally watch for two indicators of approaching obsolescence: (1) When the vendor ceases to manufacture a particular product or line of products, that is the "early warning." (2) When the vendor announces the end of maintenance support that is the "red flag" (vendors will generally give at least a one-year warning).

Media Longevity. Scientific research has yet to determine the longevity of various optical disk manufacturing processes. Even if manufacturers produce a stable and durable media, maximizing the usability of optical systems requires that special attention be paid to environmental storage conditions of the platters, copying image and index data when disks approach catastrophic failure or when a new medium is introduced, and providing for backup copies of vital data in a medium that is acceptable for archival storage.

Given that the primary goal of system migration is to maintain long-term access to optical image data, the process of accomplishing this objective may rest with a continuum of actions, including:

- a ensuring the preservation of data recorded on existing disks through careful attention to environmental storage consideration
- b maintaining the functionality of existing hardware and software through upgrades of equipment and code
- c transferring image and index data through successive versions of hardware and software
- d migrating optical imaging systems to successive technological generations, as yet undefined

There are at least three approaches to managing this continuum, each of which has advantages and disadvantages. The first approach is a continuous process of maintaining system functionality through selective equipment upgrades as the technology evolves, combined with scheduled systematic recopying of data as required. The advantage of this approach is the opportunity to work with established vendor-manufacturers, as their product lines evolve, to take advantage of the latest technological advances. In a rapidly evolving marketplace, this approach requires the least amount of clairvoyance on the part of the manager. The disadvantages of the approach are the continuous costs incurred of equipment upgrade and recopying and the necessity of depending on manufacturer stability and commitment to upgrading rather than replacing customer equipment. In a rapidly evolving marketplace, neither of these factors is certain.

The second approach to managing system migration is wholesale recopying on a periodic schedule tied to the expected longevity of the optical platter but independent of expected system life. Such a strategy assumes that hardware/software compatibility is an "uncontrollable" issue that depends more on the dynamics of the marketplace than the needs of the archives and records management community.

The advantage of the approach is that it focuses the energies of systems administrators on protecting data integrity. The disadvantage is the risk that the assumption of future systems compatibility may be a chimera.

The third approach to system migration involves transferring optical image and index data from an obsolete generation of the technology to a newly emerging generation, in some cases bypassing the generation that is becoming obsolete. In a sense this strategy "leap frogs" from the optical technology on the verge of losing its usefulness to state-of-the-art technology, which may or may not utilize optical storage media. The primary advantage of this strategy is the time it buys for systems managers while the optical imaging industry settles into a more predictable development routine or is superseded by as-yet-undeveloped technologies. The strategy places the greatest demands on system manufacturers to guarantee "backward compatibility," which is the capacity of new equipment to function similarly to the equipment it replaces, in addition to its new and different capabilities.

Adopting the leap frog strategy requires that systems managers monitor closely technology trends and not place blind faith in the future viability of the technology.

Currently it is not certain that the readability and intelligibility of optical image data in any system will be guaranteed over time without active intervention.

The primary challenge for managers responsible for managing optical image systems that must function reliably in the years ahead is to develop strategies for:

- a monitoring trends in the technological environment
- b using existing and emerging technology standards and supporting the ongoing development of data interchange standards
- c adopting prudent preservation measures in the interim

10 Optical Media Storage Systems

A digital image and optical media system is in essence a marriage of digital scanning, high density storage on optical recording material, and index retrieval technologies. The degree to which these three technologies are functionally integrated determines the effectiveness, and hence the value, of the digital image and optical media system.

Management Issues

The potential of optical imaging technology to support an agency's basic mission and improve operational efficiency may be best achieved when the technology is leveraged to enhance service, not simply used to address a single problem in isolation. Consequently, it is important that the software and hardware components of the optical system application are consistent with the information technology needs of the agency as a whole. The system's functional requirements should be assessed in terms of its storage capacity, document conversion speed, retrieval effectiveness, reliability, capacity to ensure data integrity, longevity in terms of both the optical media and the system as a whole.

These criteria should be compared and contrasted with requirements of the agency's entire community of users, including administrators, managers, and support staff.

Configuration Trends

Optical storage technology can support different imaging system configurations, from single user workstations to mainframe computers with hundreds of remote user terminals. Optical disk systems typically consist of several fundamental hardware components and optional equipment as needed:

- a system computer
- b document or film input scanner
- c optical disk drive
- d laser image printer

Optionally, systems may include index input workstations, image quality inspection, jukebox disk storage equipment, facsimile image transmission, and optical character recognition.

Early document imaging systems required extensive software development, resulting in systems with unique software capabilities. Efforts to modify or upgrade specialized systems can be difficult and time consuming, frequently requiring the involvement of the original manufacturer's software staff. Smaller stand-alone systems with proprietary software may not always accept configuration or component changes.

Optical Platter Systems

Optical media systems are commercially available in a variety of configurations, storage capacities, and data recording techniques. The three major optical platter product categories are write once/read many (WORM), rewritable, and multifunction systems. In addition, systems may be equipped with a single drive, multiple linked drives, and optical platter jukeboxes.

Write Once/Read Many (WORM) Systems

Write once, Read Many or WORM optical disks were first introduced in the early 1980's and remain a popular choice for document imaging systems. Data recorded using WORM technology is not erasable or rewritable, making WORM disks attractive for storage applications where data permanence is a primary concern. If an existing image is incorrect or no longer needed, the electronic pointer can be disabled to eliminate future retrievals at that location; new or corrected data is written to an unused area of the media. Although access to the original is blocked, the data is still on the disk and is potentially accessible. WORM optical disk selection factors include:

- a disk size (diameter in inches)
- b disk substrate (polycarbonate or tempered glass)
- c recording process (ablative, dye-polymer, thermal bubble, b-metallic, and phase-change)
- d single or dual-sided recording
- e storage capacity
- f disk durability (shelf life and post-write life)

The 5.25-inch diameter WORM systems are popular, due to factors such as: increased data storage capabilities; lower drive and media costs; less complicated jukeboxes; and, more advanced industry standards.

Larger diameter WORM media, including 12-inch and 14-inch disks, will continue to maintain broad markets in large scale document imaging environments. Laboratory research and development in areas such as laser wave lengths are also expected to further increase optical disk storage capacities, imposing additional demands on media and drive manufacturers to improve product performance and quality.

Rewritable Systems. When data permanence is of primary importance, WORM may be the technology of choice. If data is to be frequently updated, however, then rewritable optical media offer an attractive alternative. Rewritable technology offers users the ability to update recorded data as one can with magnetic hard disks. Rewritable digital optical disk media are commercially available in 3.5-inch and 5.25-inch diameters, with other formats under research and development. Although WORM systems currently are predominant, industry observers predict explosive growth of the 5.25-inch rewritable technology in the coming years. The marketplace currently offers two incompatible rewritable techniques: magneto-optical and phase change.

Magneto-Optical systems combine properties of magnetic and optical technologies. The recording or "write" process uses a laser beam to heat a premagnetized site on the media's recording surface.

This causes a reversal of the magnetic polarity, resulting in subtle reflective differences which are sensed as digital data by the "read" laser beam. The process is reversed to erase the data. A drawback of this technology is increased recording time as two passes across the disk surface are required, one to erase existing information and a second to rewrite new data. Future engineering changes are expected to correct this disadvantage. The 5.25-inch magneto-optical systems utilize two-sided media, while 3.5-inch media is one-sided.

Phase Change process alters the media's amorphous recording surface. Existing data can be erased and new data written during the same disk rotation, providing a direct data overwrite capability. Disk drives accept write once or rewritable phase change media, but industry standards have not been developed for this technology.

Multi-function Systems. Multi-function drives offer increased flexibility, accepting write-once, rewritable, and read-only optical media. Currently, users may choose between two technical approaches, since the industry has yet to adopt a single solution. One technique uses rewritable optical drives that function with either write-once or rewritable media. A second technique, using only rewritable optical media, employs special software control codes to mimic WORM functionality. Each technical approach can be evaluated on its technical merits.

Jukeboxes, or optical data libraries, are specially engineered devices for automating the storage and retrieval of optical disks. Jukeboxes typically contain at least one optical disk drive, a disk "picker" mechanism, and related computer interface controllers. When an optical disk is initially loaded in the jukebox, the disk's identifier data is read and the disk is assigned a jukebox storage location. When a disk is requested, the picker retrieves the disk and delivers it to the nearest drive. Jukebox operation is normally transparent to users; the computer system's database software automatically matches the user's query to an optical media location.

Based on user requirements, a jukebox may contain several optical drives to achieve faster data access. Due to the picker transport speeds, precise mechanical alignments are required to avoid optical media damage. Jukeboxes are available for all optical disk formats, although 5.25-inch and 12-inch jukeboxes are in greatest demand.

Due to the high development costs, they are often obtained from an existing manufacturer to ensure reliability and reduced maintenance support costs.

Document imaging systems with only a few disks or low reference requirements may not need a jukebox, relying instead on manual disk loading in a single drive. The decision to incorporate a jukebox into an optical disk system should consider planned system growth, retrieval requirements, and costs. Advantages of optical disk jukeboxes include: eliminating manual disk load and removal; increased physical security; and improved user services. Disadvantages include increased system costs for procurement, increased maintenance, and disk retrieval cycle times.

An alternative to a jukebox is a subsystem of multiple optical drives with continuously rotating disks. A network of on-line optical disks can respond almost immediately to user requests, with data retrieval dependent on the optical drive's data transfer rates. Disadvantages of these dedicated-disk multiple drive configurations include increased hardware costs and equipment maintenance.

Error Detection and Correction

Optical media technology incorporates two techniques to help guarantee that data errors are minimized on the disk as it is written and read. The first consists of powerful error correction codes that are automatically invoked to correct read errors. The second level of correction typically occurs when the error correction code software determines that the incidence of the use of error correction codes is approaching a critical point and the sector of data is automatically rewritten to another sector, which is called the relocation table.

System Integration

Document imaging systems offer benefits to organizations willing to undergo the inevitable turmoil that results from change. Maximum benefits are available when existing workflow procedures are analyzed and adapted to take advantage of the new technology, rather than just automate existing processes.

Document imaging systems vary widely in configuration, capability, and cost, reflecting the diversity of unique user needs. Early optical disk systems are not always linked with existing user information systems. Users are now requiring document imaging systems to serve as integrated operational support systems for daily operations, rather than only as off-line image repositories. Imaging systems may stretch existing computer

systems to their limits and sometimes place excess demands on electrical circuitry.

The optical disk marketplace is evolving, with an emphasis now on open systems with non-proprietary hardware components. In an open systems environment, software is the key to tying standardized system components together while retaining the flexibility needed to meet unique user needs.

Index Database Location: There are several options available for storage of the index data linked to the optical disk images. Index databases may be stored on magnetic hard disk media for improved data searching and updating. This method requires the permanent retention and periodic recopying of optical disks and magnetic media. Index data may also be stored directly on the optical media with the related images. Larger systems with specialized indexing or security requirement may find the latter approach attractive.

System Reliability and Maintenance: System component reliability is critical to system success, as prolonged or repetitive downtime can seriously erode management and user support for new imaging systems. Reliability can also be linked to system component design. For example, combining two or more optical drives in a single integrated tower configuration is a popular equipment packaging concept, providing a compact, ergonomic design compatible with desktop workstations. A disadvantage occurs when problems require the return of the equipment to the manufacturer. Unless a backup optical disk system is available, the conversion or retrieval functions may be curtailed.

Depending on the document imaging system's size and complexity, a full time, on-site maintenance technician may be required. Standard maintenance contracts may specify the scope of the technician's services as well as the responsibility of the manufacturer or vendor to supply spare and replacement parts, tools, and test equipment. An on-call contract can specify specific response time requirements. Repairs are more difficult to implement when the system consists of a collection of proprietary components integrated by a vendor who is no longer in business.

Small Computer Systems Interface: The Small Computer Systems Interface (SCSI) is one of the most important system component developments in recent years. SCSI is the primary communications interface used in optical disk systems. The ANSI X3T9.2 committee developed the intelligent parallel interface for transfer of information to and from mass storage devices such as tape, magnetic disk, and optical disk drives. Although the standard is comprehensive, much of the specific implementation of the SCSI access method has been left to local systems integrators.

As a result incompatibilities often exist at the software level among disk drives of differing manufacturers.

SCSI-2 has been developed in response to recent advances in computing technology that demand a faster interface than SCSI-1's 1.5 megabyte/second (5 megabyte/second in synchronous mode) transfer rate. Two implementations of SCSI-2 that promise data rate support two to four times (10-20 mb/s) that of its predecessor are incompatible at the hardware level. Fast SCSI communicates 8-bit data on its cable. Wide SCSI uses two cables to support 32-bit data transfer. Industry analysts feel that Fast SCSI will predominate over Wide SCSI because of lower costs and its easy adaptability to the 3.5" disk market.

Optical disk technology (including the SCSI interface) has not stabilized to the point that "one size fits all." The existence of interface standards such as SCSI-1 and SCSI-2 does not necessarily mean that all SCSI interfaces will be compatible.

A properly designed optical mass storage system can overcome this problem by including either a high-speed communications capacity or a magnetic tape drive with associated support software. Ultimately, achieving portability of media (and associated hardware) may be more difficult than guaranteeing the portability of the information itself.

11 CREATION AND USE OF TEXT INFORMATION IN AN OFFICE AUTOMATION SYSTEM

a In office automation systems which maintain the official file copy of documents on electronic media, the software shall meet the following minimum requirements:

- (1) Provide a method for all authorized users of the system to retrieve desired documents, such as an indexing or text search system;
- (2) Provide an appropriate level of security to ensure integrity of the documents;
- (3) Provide a standard interchange format when necessary to permit the exchange of documents on electronic media between computers using different software/operating systems and the conversion or migration of documents on electronic media from one system to another; and

(4) Accommodate, when necessary, the requirements for transporting permanent records to the National Archives.

b Before a document is created electronically on office automation systems which will maintain the official file copy on electronic media, each document shall be identified sufficiently to enable authorized personnel to retrieve, protect and dispose of documents in the system. Appropriate identifying information for each document maintained on the electronic media may include: office of origin, file code, key words for retrieval, addressee (if any), signatory, author, date, authorized disposition (coded or otherwise), and security classification (if applicable).

Agencies shall ensure that records maintained on such systems can be correlated with related records on paper, microform, or other media.

12 INDEXING AND LABELING ELECTRONIC RECORDS

a Electronic records will be indexed in a manner which allows the ready retrieval of their informational contents whenever necessary throughout the life cycle of the information, and which promotes the application of authorized disposal requirements. Individuals responsible for the development of electronic record systems will develop and document standardized external and internal indexing techniques for those systems. Do not assume that since the current users are very familiar with the records that no index or only a limited one is needed. Consider the likely personnel turnover in the originating office from the time the records are created until they are no longer needed for current operations.

b External indexing of electronic records includes the labeling of all off-line storage media and maintaining adequate file guides and system documentation to allow others to access the informational contents of the records when authorized.

Labels should identify, or be keyed to a file guide or system documentation which identifies;

(1) The office of primary interest (name of the organizational unit responsible for the data);

(2) The file series (system and file title(s));

(3) The time period covered by the records (dates of creation and dates of coverage);

(4) The equipment used to create the records and any devices, software, and other electronic files needed to read or decipher the information; and

(5) For certain types of electronic files, particularly those containing textual material, such as correspondence, the file guide should also identify and describe individual documents.

c Internal indexing of electronic records includes the use of a table of contents, directory, or other type of index which enables the user to identify and access a particular record without searching through the entire file of records. In some cases the internal index is generated by the system, while in other cases it must be created by the originator. The internal index must complement and be keyed to the external index, file guide, and system documentation.

d Internal indexes, or tables of contents, for diskettes or other off-line files, or for on-line files, should contain sufficient information to identify individual documents or records. If an index is not automatically generated by the equipment or the system or software being used, the originator of information on the file must create the index. Any index created by the originator should be a document accessed by a name common to all internal indexes of the electronic files of the office. For example, the index document for all records in the files of the office could be accessed by the name "INDEX". Internal indexes should contain the following information, as applicable:

- (1) Record or document name, usually not to exceed eight characters for most systems, and any other system information necessary to locate the record;
- (2) Title of official file segment;
- (3) Brief description of record or document;
- (4) Name or author of record or document; and
- (5) Dates of origination, revision(s), and final action relating to the record or document.

e The internal index should be printed out on a regular cycle, the frequency of which is dependent on the amount of updating of the file, and maintained as a file guide with other official paper records documenting the electronic records of the office.

f Indexing techniques for records in ADP systems will follow applicable Federal standards as well as accepted practices, and will be fully described in system documentation.

g External labels (or the equivalent automated tape management system) for magnetic tapes used to store permanent or unscheduled electronic records shall include the following information: name of the organizational unit responsible for the data; system and file title(s); dates of creation; dates of coverage; the recording density; type of internal labels; volume serial number, if applicable; number of tracks; character code/software dependency; information about block size; and reel sequence number, if the file is part of a multi-reel set. For numeric data files, the external label should include record format and logical record length, if applicable; data set name(s) and sequence, if applicable; and number of records for each data set.

13 FILING ELECTRONIC RECORDS FOR READY RETRIEVAL

a Electronic records are to be filed in accordance with system needs and Federal standards. The filing methods and techniques

should be fully described in the documentation of the system.

b Electronic records in an office setting should, to the extent possible, be indexed and filed in the same manner as paper records. For example:

(1) Record and nonrecord material should not be maintained on the same diskette or within the same file; instead, record material should be copied to a separate diskette or file.

(2) Diskettes and files which contain record material should be handled, duplicated, and stored in a manner which provides protection of the information from loss or change, whether inadvertent or intentional, through the use of passwords, locked file cabinets, etc.

(3) Electronic information files should be identified by the same title, and sequenced in the same way, as are similar paper or other hard copy files of the office.

14 MAINTAINING ELECTRONIC RECORDS

a Information stored on disk/diskettes has a relatively short life expectancy estimated from one to five years. Consequently, such information should be converted to another medium if it requires continued maintenance and readability.

b Permanent office correspondence such as letters, memoranda, reports, and similar correspondence should always be printed out in hard copy (paper) form or placed on approved microform (unless NARA has approved the electronic copy as the record copy) so that a copy may be filed in the office files. In addition, the legend on this file copy should include an identification of the disk/diskette on which the document is located. This will assist in retrieving the disk/diskette copy in case the document must be revised.

c Other long-term records stored on disks/diskettes should be converted to magnetic

tape, paper, microform or other appropriate media. If conversion to magnetic tape is the best alternative, the conversion process and record sequence should be coordinated with the Records Manager and NARA.

d Electronic records of long-term or permanent value should be checked periodically. The information may require transfer to new media as older media deteriorates. The following standards should be used to prevent loss of information:

(1) Agencies shall test magnetic computer tapes no more than 6 months prior to using them to store electronic records that are unscheduled or scheduled for permanent retention.

This test should verify that the tape is free of permanent errors and in compliance with National Institute of Standards and Technology or industry standards.

(2) Agencies shall maintain the storage and test areas for permanent and unscheduled computer magnetic tapes at the following temperatures and relative humidities:

Constant temperature -
62 to 68 degrees F.

Constant relative
humidity - 35% to 45%

(3) Agencies shall rewind under controlled tension all tapes containing unscheduled and permanent records every 3-1/2 years.

(4) Agencies shall annually read a 3-percent statistical sample of all permanent and unscheduled reels of magnetic computer tape to identify any loss of data and to discover and correct the causes of data loss. Tapes with 10 or more errors shall be replaced and, when possible, lost data shall be restored. All other tapes which

might have been affected by the same cause (i.e., poor quality tape, high usage, poor environment, improper handling) shall be read and corrected as appropriate.

In tape libraries with 1,800 or fewer reels, a 20% sample or a sample size of 50 reels, whichever is larger, should be read. In tape libraries with more than 1,800 reels, a sample of 384 reels should be read

(5) Agencies shall copy permanent or unscheduled data on magnetic tapes before the tapes are 10 years old onto tested and verified new tapes.

(6) Programs and system documentation must be kept for the same time as related files in order to read and retrieve the data.

(7) Reference service by Federal Record Centers normally consists of returning electronic records on a loan basis. Thus, retiring offices must keep adequate documentation for information retrieval and servicing, and keep or arrange for use of compatible equipment for display purposes until the electronic records are transferred to other media or destroyed. If this cannot be done, consider transferring permanent records to the National Archives. Long-term, non-permanent records should be written to a new system or printed out as hard copy.

e Agencies shall select appropriate media and systems for storing agency records throughout their life cycle which meet the following requirements:

(1) Permit easy retrieval in a timely fashion;

(2) Retain the records in a usable format until their authorized disposition date; and

(3) When appropriate, meet requirements for transferring permanent records to the National Archives.

f The following factors shall be considered before selecting a storage medium or converting from one medium to another:

(1) The authorized life of the records, as determined during the scheduling process,

(2) The maintenance necessary to retain the records,

(3) The cost of storing and retrieving the records,

(4) The records density,

(5) The access time to retrieve stored records,

(6) The portability of the medium (that is selecting a medium that will run on equipment offered by multiple manufacturers), and

(7) Whether the medium meets the current applicable Federal Information Processing Standards.

g The use of floppy disks shall be prohibited for the exclusive long-term storage of permanent or unscheduled electronic records.

h Agencies shall insure that all authorized users can identify and retrieve the information stored on diskettes, removable disks, or tapes by establishing or adopting procedures for external labeling.

i Agencies shall ensure that information is not lost because of changing technology or deterioration by converting storage media to provide compatibility with the agency's current hardware and software. Before conversion to a different medium, agencies must determine that the authorized disposition of the electronic records can be implemented after conversion.

j Agencies shall back up electronic records on a regular basis to safeguard against the

loss of information due to equipment malfunctions or human error. Duplicate copies of permanent or unscheduled records shall be maintained at a separate location.

k Smoking and eating shall be prohibited in magnetic computer tape storage libraries and test or evaluation areas that contain permanent or unscheduled records.

l Agencies shall issue written procedures for the care and handling of direct access storage devices which draw upon the recommendations of the manufacturers.

15 INVENTORY OF ELECTRONIC RECORDS

The inventory should include: name and control number of the records system and any implementing directives; purpose(s) and users of the system; programs and program offices supported by the system; system manager; information content of the system including major outputs; software environment; date of first input; location documentation needed to read and understand the information in the system; identification of restricted information; authorized disposition of the electronic records as determined by General Records Schedule (GRS) 20, Electronic Records, GRS 23, Records Common to Most Offices Within Agencies, or a NARA-approved records schedule; the disposition authority citation; and the location of any storage media containing permanent or unscheduled records.

16 TRANSFERRING ELECTRONIC RECORDS

a NARA and the Federal Records Centers will not accept disks/diskettes for transfer.

b They will accept magnetic tapes/tape cartridges provided:

(1) They are covered by an approved records disposition schedule or, in the case of permanent, historically valuable records, are offered directly to NARA.

(2) The file recorded on the tape is inactive or the creating office cannot provide proper care and handling of the tape to ensure the preservation of the information it contains.

(3) Tapes to be transferred to an FRC or NARA shall be on one-half inch 7 or 9 track tape reel to reel magnetic tape, written in ASCII or EBCDIC, with all extraneous control characters removed from the data (except record length indicators for variable length records, or marks designating a datum, word, field, block or file), blocked no higher than 30,000 bytes per block, at 800, 1600 or 6250 bpi.

Additionally, agencies are authorized to transfer permanent electronic records to the National Archives on 3480 class tape cartridges that meet the American National Standard based on the IBM format.

The magnetic tape and cartridge for information interchange must be 18-track, parallel, 12.65 mm (1/2 inch), and 1491 cpmm (37, 871 cpi).

All maintenance requirements of 36 CFR 1234.28(g) apply to 3480 class tape cartridges. NARA will copy the contents of 3480 class tape cartridges at the time of accessing and return them to the agency unless the agency indicates that it does not want the cartridges returned.

(4) The tapes shall be new or recertified tapes which have been over a tape cleaner before writing and shall be rewound under controlled tension.

(5) Documentation adequate for servicing and interpreting the records shall be transferred with them. The documentation shall include, but is not limited to a completed Standard Form 277, Computer Magnetic Tape File Properties, or its equivalent; and the code book specifications defining the data elements and their value that match the new format of the data where applicable. If the specifications are contained in an automated data

element dictionary, hard copy from that system will suffice.

c NARA and the FRC's will also accept microfilm, computer output microfilm, and other microforms provided the standards in 41 CFR 101-11.5 are adhered to. Operating activities planning to transfer microform copies of electronic records should consult their Records Manager.

17 SECURITY OF ELECTRONIC RECORDS

a Special precautions may be needed to ensure the security of electronically stored information. To determine the level of security protection required, safeguards should be selected on the basis of risk analyses and security reviews, standards, and guidelines. Document these safeguards in agency and facility security plans. (See DM 3140-1). Security should be a major determinant in evaluating use of microcomputers or personal computers, particularly in a network environment.

When microcomputers are used as terminals communicating with host computers, all security features provided by the host must be used; access keys to the host computer must be protected and passwords changed frequently

(DR 3130-2).

b Agencies having electronically stored information are responsible for ensuring that data integrity is maintained. This includes, but is not limited to, protecting electronic records against unauthorized destruction and taking steps, in coordination with their Records Manager, to ensure:

- (1) That all their electronic records are covered under an approved records disposition schedule;
- (2) That only authorized personnel have access to electronic records;
- (3) That their electronic record systems provide for continuity of support should their normal operations be disrupted in an

emergency, and provide for adequate back-up and recovery of records to protect against information lost;

(4) That appropriate agency personnel are trained to safeguard sensitive or classified electronic records;

(5) That the unauthorized alteration or erasure of electronic records is prevented;

(6) That electronic records security is included in computer systems security plans proposed pursuant to the Computer Security Act of 1987;

(7) That electronic records scheduled for destruction are disposed of in a manner that ensures protection of any sensitive, proprietary, or national security information;

(8) That magnetic recording media previously used for electronic records containing sensitive, proprietary, or national security information are not reused if the previously recorded information can be compromised by reuse in any way; and

(9) Processing of USDA information on employee-owned equipment must be authorized by the appropriate agency management (DR 3140-1).

18 DISPOSAL OF ELECTRONIC RECORDS

a The processing elements for the disposition phase of the life cycle of electronic information are the same as for records in any other media, i.e., storage, transfer, preservation, and destruction. Certain requirements, however, are unique to the use of specific information technologies. It is not the physical form of the record that determines its retention and disposal action but the content of the information and its use. As with paper records, electronic records can only be disposed of according to an approved

agency records control schedule or a General Records Schedule. In addition, personnel should follow the agency's established procedures for the systematic disposal of records.

b Permanent electronic records will be maintained in accordance with the requirements of NARA regulations, and will be converted to paper, microfilm, or other media approved by the Archivist of the United States for the retention of archival records. Such records, along with adequate documentation and adjunct files to permit access to them, will be transferred to the National Archives as soon as possible when it is determined that the agency cannot or does not wish to continue maintaining the records.

c Electronic records eligible for destruction will be destroyed by erasing, degaussing, or overwriting. Use of a "delete", "erase", or similar key (depending on type and brand of equipment) may not actually destroy the information, but will only make it unretrievable through use of the normal system access methods. It can still be retrieved through use of special software.

d Electronic records will not be kept beyond their authorized retention periods.

19 JUDICIAL USE OF ELECTRONIC RECORDS

a Properly created and maintained electronic records pose no greater legal problems than do paper or micrographic records, unless there are specific statutory or regulatory requirements for paper records (as may be the case with certain medical records, for example). The Federal Rules of Evidence (Rule 803 (8)) provide that official records may be admitted as evidence for the activity. The text of the rule is: "The following are not excluded by the hearsay rule, even though the declarant is available as a witness:

***** (8) Public records and reports--Records, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth (A) the activities of the office or agency, or (B) matters observed pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel,

or (C) in civil actions and proceedings and against the Government in criminal cases, factual findings resulting from an investigation made pursuant to authority granted by law, unless the sources of information or other circumstances indicate lack of trustworthiness."

b Under this rule, if the only record is electronic, agencies must ensure that procedures are established and followed so that:

(1) The date of the record can be determined;

(2) The date of any alterations will be automatically recorded by the system; and

(3) It will be evident that the document was authorized to be issued ("signed") by an appropriate agency official.

If these steps are not taken, the trustworthiness of the record could easily be called into question, and it could be refused as evidence. Contact OGC for specific advice.

c The following procedures can also enhance the admissibility in legal proceedings of electronic records:

(1) Documentation that similar kinds of electronic records are created by the same processes and have a standardized retrieval approach;

(2) Substantiation that security procedures prevent unauthorized modification of a record and ensure system protection against such problems as power interruptions; and

(3) Identification of the electronic media on which records are stored throughout their life cycles, the maximum time span that records remain on each storage medium, and the NARA-approved disposition of all records.

d If a vital record is kept in electronic form, document the vital records procedures, including a description of the informational content of the various generations; i.e., the original and vital record copies.

20 ADMISSIBILITY OF ELECTRONICALLY FILED FEDERAL RECORDS AS EVIDENCE

Recognizing that electronically filed Federal records are subject to being offered as evidence in litigation, these guidelines have been prepared to familiarize Federal program managers, as well as record custodians, with the rules of evidence as they apply to such records. It is also intended to serve as a refresher for their legal counsel. This familiarization should assist in establishment of appropriate procedures in creating and maintaining electronically filed records that will assure their admissibility in court proceedings and enhance their probative value as reliable and trustworthy representations of their purported contents.

Introduction

Electronically filed records are by their nature machine readable, they, therefore, fall within the statutory definition of Federal records.

Because electronically filed Federal records are subject to being offered as evidence to support the government's contention in litigation, precautions should be taken to assure their admissibility and probative value. Presented herein are: 1) a compilation of Federal Rules of Evidence and statutory provisions that are particularly relevant in offering such evidence for admission in Federal court; and 2) requirements for laying a proper foundation for its admissibility. The discussion is directed to managers or custodians of electronically filed Federal records. It is intended to provide guidance that will assure proper procedures are followed that will preserve the "trustworthiness" of these records as evidence.

It should be noted that the rules of evidence are no different for electronically filed records than for paper records. However, because electronic files are particularly susceptible to purposeful or accidental alteration, or incorrect processing, laying a foundation for their admission must be done with particular care. Proper control over creation and maintenance of these files can be crucial in overcoming objections that will be raised in the courtroom. Although creation and maintenance of electronic files inherently imposes strict procedural controls, inadequate documentation or inability to explain these controls in laymen's terms can have dire consequences either in getting such evidence admitted or in the weight it is accorded in terms of probative value.

The Best Evidence Rule, Hearsay and Authentication

The filing of records electronically means to store computer processed information in storage media such as magnetic disks or tapes, where the information is represented in the storage media in the form of "machine readable" codes or patterns imprinted on magnetizable surfaces by electronic impulses. In the case of optical disk files (e.g., CD-ROM), the information is, in most instances, "etched" on the surface of a specially coated disk with a laser beam. Although the information stored on an optical disk is in effect a bit-pattern "image" of optically scanned literal, graphic or pictorial information (as opposed to binary-coded characters), it is nonetheless "machine-readable" and, in the absence of statutory or case law to the contrary, should be treated no differently than information stored on magnetic disk or tape regarding its admissibility and trustworthiness.

(In fact, an argument could be made that read-only files are more trustworthy!)

Although the information is "filed" electronically in these media, the files themselves are in reality magnetic files. In any case, such files are considered "writings or recordings" in Federal courts.

Federal Rules of Evidence, Rule 1001(1) states in pertinent part: "Writings and recordings" consist of letters, words, or numbers, or their equivalent, set down by...magnetic impulse, mechanical or electronic recording, or other form of data compilation.

(1) The Best Evidence Rule

Magnetic files are called "machine readable" because they can be copied into a computer for processing and interpreted for printing in human readable form on paper or microfilm, or on a video display screen. Before the courts, an "original" of a record is the record itself, which can pose a problem regarding computer printouts in the face of the "best evidence rule." This rule, when rigidly applied, precludes admissibility of anything but the original document to prove its content.

Recognizing the impracticality of this rule when applied to magnetic files, many states and the Federal government have adopted rules that define computer printouts as original, provided that they have been shown to accurately reflect the information in the magnetic files. Federal Rules of Evidence, Rule 1001(3) states in pertinent part: An "original" of a writing or

recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original."

Absent such a rule, at least one court has taken the view that printouts of records stored in magnetic media are admissible because they are "unavailable and useless except by means of the printout sheets."

Federal rule of Evidence 1002 states that "to prove the content of a writing, recording or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress." The Federal Rules of Evidence do indeed provide otherwise. With regard to duplicates and public or official records, the rules state in pertinent part as follows:

A "duplicate" is a counterpart produced by the same impression as the original,.... or by mechanical or electronic re-recording,... or by other equivalent techniques which accurately reproduce the original. Federal Rule of Evidence 1001(4).

A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original. Federal Rule of Evidence 1003.

The contents of an official record, or of a document authorized to be filed and actually recorded or filed, including data compilations in any form, if otherwise admissible, may be proved by copy, certified by a witness who has compared it with the original. If a copy which complies with the foregoing cannot be obtained by the exercise of reasonable diligence, then other evidence of the contents may be given. Federal Rule of Evidence 1005.

These rules would seem to consider as duplicates, or copies of official records, additional printouts of the same information contained in a magnetic file produced at different times, as well as carbon, photostatic or xerographic copies.

U.S. Code Title 28, SEC. 1732 (commonly known as the Business Records Act) provides for admissibility of copies or reproductions of original records produced in the regular course of business. This section states in pertinent part:

If any...department or agency of government, in the regular course of business or activity has kept or recorded any memorandum, writing, entry, print, representation or combination thereof, of any act, transaction, occurrence, or event, and in the regular course of business has caused any or all of the same to be recorded, copied, or reproduced by any..process which accurately reproduces or forms a durable medium for so reproducing the original, the original may be destroyed in the regular course of business unless its preservation is required by law. Such reproduction, when satisfactorily identified, is as admissible in evidence as the original itself in any judicial or administrative proceeding whether the original is in existence or not... . The introduction of a reproduced record...does not preclude admission of the original.
....

(Federal Rule of Evidence 803(6), stated below, closely parallels the Business Records Act.)

U.S. Code Title 28, SEC. 1733 is pertinent regarding government records and papers that may be electronically filed with the caveat that it is superseded by the Federal Rules of Evidence. The section states:

(a) Books or records of account or minutes of proceedings of any department or agency of the United States shall be admissible to prove the act, transaction, or occurrence as a memorandum of which the same were made or kept.

(b) Properly authenticated copies or transcripts of any books, records, papers or documents of any department or agency of the United States shall be admitted in evidence equally with the original thereof.

(c) This section does not apply to cases, actions, and proceedings to which the Federal Rules of Evidence apply.

(2) Hearsay

As was pointed out earlier, a computer printout is regarded as an original writing or recording. A computer printout offered to prove the truth of its contents is considered hearsay.

Federal Rule of Evidence 801(c) defines hearsay as "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." A "statement" is defined to include a written assertion. Federal Rule of Evidence 801(c).

Hearsay is not admissible in Federal court except as provided by the Federal Rules of Evidence "or by other rules prescribed by the Supreme Court pursuant to statutory authority or by Act of Congress." Federal Rule of Evidence 802.

Among the exceptions enumerated in Federal Rule of Evidence 803 that are particularly relevant to computer printouts are the following, stated in pertinent part:

The following are not excluded by the hearsay rule, even though the declarant is available as a witness:

(a) Records of regularly conducted activity

A memorandum, report, record, or data compilation, in any form, or

acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method of circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

(b) Absence of entry in records kept in accordance with the provisions of paragraph (1)

Evidence that a matter is not included in the memorandum, reports, records, or data compilations, in any form, kept in accordance with the provisions of paragraph (1), to prove the nonoccurrence or nonexistence of the matter, if the matter was a kind which a memorandum, report, record, or data compilation was regularly made and preserved, unless the sources of information or other circumstances indicate lack of trustworthiness.

(c) Public records and reports

Records, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth (A) the activities of the office or agency, or (B) matters observed pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel, or (C) in civil actions and

proceedings and against the Government in criminal cases, factual findings resulting from an investigation made pursuant to authority granted by law, unless the sources of information or other circumstances indicate lack of trustworthiness.

(d) Absence of public record or entry

To prove the absence of a record, report, statement, or data compilation, in any form, or the nonoccurrence or nonexistence of a matter of which a record, report, statement, or data compilation, in any form, was regularly made and preserved by a public office or agency, evidence in the form of a certification in accordance with rule 902, or testimony, that diligent search failed to disclose the record, report, statement, or data compilation, or entry.

(3) Authentication

Any tangible thing offered as evidence is subject to challenge regarding its genuineness. Computer printouts are no exception. Federal Rule of Evidence 901(a) states:

The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

Federal Rule of Evidence 901(b) lists examples of authentication by way of illustration, including the following that are particularly pertinent to the admissibility of computer printouts.

(a) Testimony of witness with knowledge

Testimony that a matter is what it is claimed to be.

...

(b) Public records or reports

Evidence that a writing authorized by law to be recorded or filed and in fact recorded filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.

(c) Ancient documents or data compilation

Evidence that a document or data compilation, in any form, (A) is in such condition as to create no suspicion concerning its authenticity, (B) was in a place where it, if authentic, would likely be, and (C) has been in existence 20 years or more at the time it is offered.

(d) Process or system

Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

(e) Methods provided by statute/or rule

Any method of authentication or identification provided by Act of Congress or by other rules prescribed by the Supreme Court pursuant to statutory authority.

Certain documents or records (including computer printouts) are self-authenticating, as provided in Federal Rule of Evidence 902, which states in pertinent part:

Extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:

(1) Domestic public documents under seal

A document bearing a seal purporting to be that of the United

States, or of any State, district, Commonwealth, territory, or insular possession thereof, or of the Panama Canal zone, or the Trust Territory of the Pacific Islands, or of a political subdivision, department, officer, or agency thereof, and a signature purporting to be an attestation of execution.

(2) Domestic public documents not under seal

A document purporting to bear the signature in his official capacity of an officer or employee of any entity included in paragraph (1) hereof, having no seal, if a public officer having a seal and having official duties in the district or political subdivision of the officer or employee certifies under seal that the signer has the official capacity and that the signature is genuine.

(3) Certified copies of public records

A copy of an official record or report or any entry therein, or of a document authorized by law to be recorded or filed and actually recorded or filed in a public office, including data compilations in any form, certified as correct by the custodian or other person authorized to make the certification, by certificate complying with paragraph (1), (2), or (3) of this rule or complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority.

(4) Official publications

Books, pamphlets, or other publications purporting to be issued by public authority.

(5) Acknowledged documents

Documents accompanied by a certificate of acknowledgement

executed in the manner provided by law by a notary public or other officer authorized by law to take acknowledgements.

....

(6) Presumptions under Acts of Congress

Any signature, document, or other matter declared by Act of Congress to be presumptively or prima facie genuine or authentic.

21 SPECIAL CONSIDERATIONS

In 1986, Congress reauthorized the Rehabilitation Act of 1973, as amended (Public Law 99-506, 29 U.S.C. 794d). Section 508, as incorporated into the Act, mandates that guidelines be established to ensure that handicapped individuals may use electronic office equipment with or without special peripherals, and that agencies comply with these guidelines when acquiring electronic equipment.

FIRMR Bulletin C-8, dated 1/30/91, provides information and guidance regarding agencies' responsibility to meet the special Federal information processing (FIP) resource accommodation needs of individuals with disabilities.

FIRMR Bulletin C-10, Telecommunication accessibility for hearing provides guidelines for acquiring products and services that provide telecommunication accessibility for hearing and speech impaired individuals for communication with and within Federal agencies. This bulletin also provides general information regarding responsibilities for accommodating the needs of those with hearing and speech impairments.

Summation

Refer to the FIRMR bulletin for further guidance on the subject. One may contact the USDA "The Technology Accessible Resources Give Employee Today (TARGET) Center, room 1006-S Bldg., telephone (Voice/TDD): 202-720-2600.

General Terms

Accessibility. Workstations for employees with sensory, cognitive, or mobility impairments may be equipped with special peripherals or software that provide access to computer technology, primarily microcomputers.

Equivalent access. Disabled individuals and nondisabled individuals should be provided equivalent access to electronic office equipment. FIP resources, particularly microcomputers, provide enhancement features, such as text enlarging and speech input and output, allowing disabled individuals to accomplish tasks previously impossible for them. For example, the inherent flexibility of microcomputers permits their adaptation to meet the specific needs of disabled individuals through the use of braille printers, spoken screen review, and keyboard replacement devices.

Functional specifications. Are organized by functional requirement into three categories: input, output and documentation. These specifications reflect the major areas that need to be considered during planning and acquisition.

Accessibility alternatives. Accessibility solutions range from third-party hardware and software add-ons, such as "layered" solutions, to hardware "built-ins" and operating system enhancements. Agencies should attempt to provide the same equipment to all of their employees, whether or not they are disabled. For that reason, "built-in" accessibility solutions are preferable to "layered" solutions. Layering involves adding layers of software between the end-user and the operating system or application software. While this often complex solution may have advantages, such as increased function and performance, it can also have serious disadvantages. Disadvantages include increased costs, greater difficulty in maintaining software updates at the operating system level, and increased costs to train employees to utilize dissimilar equipment at different sites within the agency. For these reason, layering should be selected as an accessibility solution only after careful analysis of its merits relative to that of "built-in" solutions.

Acronyms

COCA - Clearinghouse on Computer Accommodation

DSO - Designated Senior Official

TARGET - Technology Accessible Resources Gives

Employment Today

CONCLUSION

The introduction of electronically filed records as evidence can be difficult because of the avenues open for challenging their relevance and reliability. Common assaults on the integrity of computer stored or generated files include questioning:

- 1) the source of the input data or information and the process for transcribing it to machine readable form;
- 2) the computer programs that create, edit and update the files;
- 3) the computer programs that produce the output or stored files; and
- 4) the reliability of the hardware and vendor-supplied "off-the-shelf" software that systematically manages the internal processes of the computer.

The increasing use of computers in creating and maintaining records in the ordinary course of business has resulted in the courts' tending to treat printouts of electronically stored "business" records no differently than other records. However, the increased complexity of safeguarding the integrity of computer files accessible through remote terminals can dampen this tendency.

In any event, computer records not offered as business records will continue to present special foundation problems often requiring the testimony Of technical experts.

It is the purpose of this guideline to provide an understanding of the rules of evidence as they apply to electronically filed records in order that appropriate agency procedures are instituted in creating and maintaining such records. Of particular importance is that Federal records managers or custodians assure the existence of up-to-date documentation that fully and accurately describes the procedural controls employed. Additionally, records managers or custodians must be prepared to describe these controls in laymen's term and to account for each link in the chain of events involved in producing the records.

Apart from the requirements of the rules of evidence, preserving the integrity of Federal records in general is an inherent responsibility of anyone charged with their keeping.

Signed by:

JOHN L. OKAY

END